2. What are the Different Types of Advanced Port Scans?

In **advanced port scanning with Nmap**, there are several types of scans beyond the basic port scan. Each type provides unique insights, from finding open ports in stealthy ways to revealing more information about the target's operating system or services. Here's a breakdown of the main types:

---

1. SYN Scan (Stealth Scan)

- **Command:** `nmap -sS <target>`
- **Description:** Sends SYN packets to initiate but not complete the TCP handshake, making it stealthier and less likely to be logged. SYN scans are quick and can bypass certain firewalls and intrusion detection systems.

2. TCP Connect Scan

- **Command:** `nmap -sT <target>`
- **Description:** Completes the full TCP handshake, making it easier to detect. Often used when SYN scans require root privileges or aren't allowed.

3. UDP Scan

- **Command:** `nmap -sU <target>`
- **Description:** Scans for open UDP ports, often used for discovering services like DNS (port 53) and SNMP (port 161). UDP scans can be slower due to the protocol's stateless nature and can be harder to detect.

4. ACK Scan

- **Command:** `nmap -sA <target>`
- **Description:** Used for **firewall and filtering analysis** rather than port discovery. Sends ACK packets to determine if a firewall is stateful or stateless and to identify filtered ports.

5. Window Scan

- **Command:** `nmap -sW <target>`
- **Description:** Similar to ACK scan but relies on TCP window size variations to infer open ports. Not all systems respond in ways that make this scan effective, but it can be useful in some cases.

6. FIN Scan

- **Command:** `nmap -sF <target>`
- **Description:** Sends FIN packets without opening a connection, attempting to bypass firewalls and IDS. If the port is closed, the target responds with an RST (reset packet), but open ports are

typically silent.

7. XMAS Scan

- **Command:** `nmap -sX <target>`
- **Description:** Sends a packet with all flags set (XMAS tree pattern). Similar to the FIN scan, it exploits systems' responses to unexpected packets to infer open and closed ports. Effective against some firewalls and older systems.

8. NULL Scan

- **Command:** `nmap -sN <target>`
- **Description:** Sends packets with no TCP flags set. Like FIN and XMAS scans, it checks for ports by observing RST responses from closed ports. NULL scans are useful for identifying systems that respond differently to empty packets.

9. Idle (Zombie) Scan

- **Command:** `nmap -sI <zombie_host> <target>`
- **Description:** Uses a third-party "zombie" host to send packets, making it appear as if the scan is coming from the zombie host. This allows highly stealthy scans with no direct contact between the scanner and the target.

10. IP Protocol Scan

- **Command:** `nmap -sO <target>`
- **Description:** Checks which IP protocols (e.g., ICMP, TCP, UDP) are supported on the target, allowing detection of protocols that might be available beyond the standard TCP/UDP port scans.

11. SCTP INIT Scan

- **Command:** `nmap -sY <target>`
- **Description:** Used for **Stream Control Transmission Protocol (SCTP)** networks, commonly found in telecom networks. The scan sends INIT chunks to initiate communication, helping to identify SCTP services on the target.

12. SCTP Cookie Echo Scan

- **Command:** `nmap -sZ <target>`
- **Description:** An SCTP-specific scan that bypasses the normal handshake, attempting to discover open SCTP ports without the full connection.

13. Service Version Detection

- **Command:** `nmap -sV <target>`
- **Description:** Goes beyond basic port scanning to identify the software and version running on open ports. This can reveal potential vulnerabilities associated with specific versions.

14. OS Detection

- **Command:** `nmap -O <target>`
- **Description:** Attempts to identify the target's operating system based on packet responses, often providing details about the kernel and OS version.

15. Timing and Fragmentation Scans

- **Command:** `nmap -f` (for fragmentation) or `-T0` to `-T5` (for timing)
- **Description:** Uses timing options to adjust scan speed and fragmentation to break packets into smaller chunks, helping evade firewalls and IDS by being either stealthy or fragmented enough to bypass detection.

16. NSE (Nmap Scripting Engine) Scans

- **Command:** `nmap --script=<script> <target>`
- **Description:** Nmap's scripting engine allows for **custom scripts** that can detect vulnerabilities, brute force services, gather information, and much more. NSE scripts can be used for basic information gathering to complex vulnerability exploitation.
- **Popular Scripts:**
  - `vuln` (vulnerability detection)
  - `brute` (brute-forcing)
  - `malware` (malware scanning)
  - `safe` (non-intrusive scans for general information)

Using Multiple Techniques Together

You can combine several scan types to perform more thorough reconnaissance, like this example command:

```
nmap -sS -sU -sV -O -p 1-1000 --script=vuln <target>
```

This performs:

1. A **SYN scan** (`-sS`),
2. A **UDP scan** (`-sU`),
3. **Version detection** (`-sV`),
4. **OS detection** (`-O`),
5. **Port range** 1-1000 (`-p 1-1000`), and
6. **Vulnerability scanning** using the `vuln` script (`--script=vuln`).

Key Takeaways

- **Stealth Scans** like SYN and ACK are useful for evading detection.

- **TCP/UDP Combined Scans** help identify both types of services.
- **NULL, FIN, and XMAS Scans** are useful for detecting filtered ports on systems that respond uniquely.
- **Idle (Zombie) Scans** allow indirect scanning, useful for stealth.
- **NSE Scans** add flexibility for in-depth exploration with scripts.